UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/500,869	02/09/2000	Semyon B Mizikovsky		3161

7590 03/18/2004

Docket Administrator (Rm 3C-512)
Lucent Technologies Inc
600 Mountain Avenue P O Box 636
Murray Hill, NJ 07974-0636

EXAMINER
HO, THOMAS M

ART UNIT	PAPER NUMBER
2134	5

DATE MAILED: 03/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/500,869	**Applicant(s)** MIZIKOVSKY, SEMYON B	
	Examiner Thomas M Ho	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 October 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12/22/03* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1. The amendment of October 2nd, 2003 has been received and entered.

Response to Amendments

2. Applicant's arguments, see page 10, filed October 2nd, 2003, with respect to the rejection(s)of claim(s) 1-15 under 35 Patel USC 102 and 35 USC 103 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Patel.

3. Claims 1-18 are pending.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-18 are rejected as being anticipated by Patel.

In reference to claim 1:

Patel(Column 4, lines 1-60) discloses a method of updating a communications key maintained in a unit for communicating with a communications system, said method comprising:

- Generating a new communications key using a secret value stored in said unit, where the new communications key is the SSD. (Column 4, Lines 58-62)
- Generating an update key using said secret value stored in said unit, where the update key is M-key. (Column 4, Lines 1-6)
- Generating a signature value using said update key, where the signature that is generated is $KCF_{M\text{-}Key}$(Rm, Rn, Type, 0) or $KCF_{M\text{-}Key}$ (Rm, Type, 1) (Column 4, Lines 23-32)
- Comparing said signature value with a signature value received from a visiting communications system of said communications system which was generated by said visiting communications system using said update key derived by a home communications system of said communications system, where the update key that is derived by the home communication system is M-key and the signatures that are compared $KCF_{M\text{-}Key}$(Rm, Rn, Type, 0) are used to authenticate a party. (Column 4, Lines 43-48)
- Updating said communications key with said new communications key depending on the results of said comparison, where the SSD is only updated if both parties can be authenticated. (Column 4, Lines 58-62)

In reference to claim 2:

Patel(Column 4, lines 1-60) discloses the method of claim 1 comprising:

- Receiving an update sequence, where the update sequence is received by the Mobile unit. (Column 4, Lines 20-24)
- Generating said new communications key using a secret value stored in said unit and said update sequence, where the new communications key SSD is generated using several secret values, Rm, Rn, A-key, M-Key, and the update sequence which is used in the KCF calculation as the input "Type". (Column 4, Lines 51-62)

In reference to claim 3:

Patel(Column 4, lines 1-60) discloses the method of claim 2 further comprising:

- Generating a challenge sequence, where the challenge sequence is Rn. (Column 4, Lines 20-29)
- Sending said challenge sequence to said visiting communications system, where Rn is sent to the mobile. (Column 4, Lines 20-29)
- Generating said signature value using said challenge sequence and said update key, where the mobile unit generates the signature value $KCF_{M\text{-}Key}$(Rm, Rn, Type, 0) from the challenge sequence Rn and the update key M-Key. (Column 4, Lines 23-32)
- Receiving said signature string generated by said visiting communications system using said challenge sequence and said update key, where the AC/HLR receives this signature string $KCF_{M\text{-}Key}$(Rm, Rn, Type, 0). (Column 4, Lines 43-47)
- Comparing said signature value with said signature value generated by said visiting communications system, where the AC/HLR compares the signature value $KCF_{M\text{-}}$

$_{\text{Key}}$(Rm, Rn, Type, 0) with its own computation of it to authenticate the mobile. (Column 4, Lines 43-48)

In reference to claim 4:

Patel(Column 4, lines 1-60) discloses the method of claim 3 comprising:

- Generating a second signature value using said update sequence and said update key, where the second signature value is KCF$_{\text{M-Key}}$ (Rm, Type, 1). (Column 4, lines 46-50)
- Sending said second signature value to said visiting communications system for comparison with a second signature value generated by said visiting communications system using said sequence and said update key generated at said communications system, where the second signature value KCF$_{\text{M-Key}}$ (Rm, Type, 1) is sent off and compared with the KCF$_{\text{M-Key}}$ (Rm, Type, 1) generated at the mobile unit to authenticate the network. (Column 4, Lines 46-57)

In reference to claim 5:

Patel(Column 4, lines 1-60) discloses the method of claim 3 wherein said generating said signature value includes:

- Developing a signature string comprising at least portions of said update sequence, said challenge sequence and said update key, where a signature string is any number of possible intermediate values in the computation of KCF$_{\text{M-Key}}$(Rm, Rn, Type, 0). These intermediate values which must be generated are inherent to the KCF function, which is an HMAC, but could be a PRF such as DES-CBC.

- Generating said signature value from at least said signature string, where the final computation is the signature value $KCF_{M\text{-}Key}$(Rm, Rn, Type, 0).

The examiner notes that KCF may be an HMAC or a DES-CBC, which computes its final result through a series of rounds and inputs, where the output of one round is inputted into the input of the next round.

In reference to claim 6:

Patel(Column 4, lines 1-60) discloses the method of claim 4 wherein said generating said signature value includes:

- Developing a second signature string comprising at least portions of said update sequence, said challenge sequence and said update key, where the second signature string can be any number of the intermediate values or computations in the function $KCF_{M\text{-}Key}$ (Rm, Type, 1). These intermediate values which must be generated are inherent to the KCF function, which is an HMAC, but could be a PRF such as DES-CBC.
- Generating said second signature value from at least said second signature string, where the final result of the function is $KCF_{M\text{-}Key}$ (Rm, Type, 1), the second signature value.

The examiner notes that KCF may be an HMAC or a DES-CBC, which computes its final result through a series of rounds and inputs, where the output of one round is inputted into the input of the next round.

In reference to claim 7:

Patel(Column 1, Line 40 – Column 2, line 58) discloses a method of updating a communications key maintained in a unit and in a communications system, said method comprising:

- Receiving by a visiting communications system from a home communications system an update sequence and an update key derived by said home communications system using a secret value associated with said unit and stored in said home communications system, where the visiting communications system is the VLR, the home communications system is the AC/HLR, and the unit is the mobile unit. The VLR receives an update sequence, SR, and the update key SSDA using the secret data RANDSSD from the home communications system the AC/HLR. (Column 2, Lines 22-30)
- Sending by said visiting communication system to said unit said update sequence for said unit to generate a new communications key using a secret value in said unit, where the VLR sends the update sequence to the mobile. (Column 2, lines 29-33)
- Generating a signature value at said visiting communications system using said update key derived by said home communications system, where the signature value generated is $\text{CAVE}_{\text{SSDA}}$(Rm) and the update key derived by the AC/HLR is SSDA. (Column 2, lines 43-46)
- Sending by said visiting communications system to said unit said signature value generated at said visiting communications system for said unit to compare with a signature value generated at said unit using an update key generated by said unit using said secret value stored in said unit, where the VLR sends the signature value

$CAVE_{SSDA}(Rm)$ to the unit, where the unit makes a comparison to authenticate the network. (Column 2, Lines 42-46)

- Receiving an update confirmation depending on the results of said comparison, where the update confirmation is a signal indicating verification. (Column 2, lines 47-48)

Claim 8 has been canceled.

In reference to claim 9:

Patel(Column 1, Line 40 – Column 2, line 58) discloses the method of claim 7 wherein said generating a signature value including:

- Receiving a challenge sequence from said unit, where the challenge sequence received from the unit is Rm. (Column 2, Lines 35-38)
- Generating said signature value using said challenge sequence and said update key, where the signature value is generated using the challenge sequence Rm, and the update key SSDA as $CAVE_{SSDA}(Rm)$. (Column 2, lines 43-46)

In reference to claim 10:

Patel(Column 1, Line 40 – Column 2, line 58) discloses the method of claim 9 including:

- Generating a second signature value using said update sequence and said update key, where the second signature value is $CAVE_{SSDA}(Rn)$. (Column 2, lines 50-52)
- Receiving a second signature value generated at said unit using said update sequence and said update key at said unit, where the second signature value is $CAVE_{SSDA}(Rm)$, where

$CAVE_{SSDA}(Rm)$ is generated in the mobile unit, and the update key is SSDA. (Column 2, lines 50-52)

- Comparing with said second signature value with said second signature value generated by said unit, where the second signature $CAVE_{SSDA}(Rm)$ is generated in the mobile and received by the VLR to be compared. (Column 2, lines 48-54)

In reference to claim 11:

Patel(Column 1, Line 40 – Column 2, line 58) discloses the method of claim 10 wherein said generating a signature value including:

- Developing a signature string comprising at least portions of said update sequence, said challenge sequence and said update key, where the signature value is generated from the update sequence, challenge sequence, and update key, and where the signature string is any one of the intermediate values, which are inherent to the computation of the signature value, $CAVE_{SSDA}(Rm)$.

In reference to claim 12:

Patel(Column 1, Line 40 – Column 2, line 58) discloses the method of claim 10 wherein said generating a second signature value including:

- Developing a second signature string comprising at least portions of said update sequence, said challenge sequence and said update key, where the signature value is generated from the update sequence, challenge sequence, and update key, and where the signature string is any one of the intermediate values, which are inherent to the computation of the signature value, $CAVE_{SSDA}(Rm)$.

In reference to claim 13:

Patel(Column 1, Line 40 – Column 2, line 58) discloses a method of updating a communications key maintained in a unit and in a communications system, said method comprising:

- Generating an update sequence, where the update sequence is the session request SR, instructive of the mobile unit to perform the update protocol. (Column 4, lines 29-34)
- Generating by a home communications system a new communications key using a secret value stored in said home communications system and associated with said unit, where the new communications key is a new session key generated using the secret values RANDSSD, Rn, Rn, SSDA, SSDB. (Column 2, lines 57-58)
- Generating by said home communications system an update key using said secret value (Column 2, lines 23-27), where the update key is SSDA.
- Sending said update key to a visiting communications system for said visiting communications system to generate a signature value which is sent to said unit for comparison to a signature value generated at said unit using an update key generated at said unit using a secret value stored in said unit, where the update key is sent to the VLR by the AC/HLR, whereupon the VLR generates $CAVE_{SSDA}(Rm)$ to be sent to the unit which in turn generates $CAVE_{SSDA}(Rm)$ to compare the two. (Column 2, Line 26)

- Updating said communications key with said new communications key depending on the results of said comparison, where the keys are updated only if the comparison was matched and the parties had successfully authenticated. (Column 2, lines 57-58)

Claim 14 has been canceled.

In reference to claim 15:

Patel(Column 4, lines 1-60) discloses a method of updating a communications key maintained in a unit and in a home communications system, said method comprising:

- Receiving an update sequence from said home communications system for said unit to generate a new communications key using a secret value in said unit, where the update sequence is SR, the home communications system is the AC/HLR, and the new communications key is SSD. (Column 4, lines 20-24)
- Receiving an update key from said home communications system and generated at said home communications system using a secret value associated with said unit at said home communications system, where the update key is the Rn, generated at AC/HLR.
- Performing an authentication with said unit using said update sequence, where the update sequence or TYPE, indicative of the update protocol. (Column 4, lines 55-62)
- Sending to said home communications system the results of said authentication, where the results are understood to be known to the home communications system so it knows whether or not to complete the update protocol. (Column 4, lines 55-62)

In reference to claim 16:

Patel(Column 1, Line 40 – Column 2, line 58) discloses a communications key update system for updating a communications key maintained in a unit for communicating with a communications system, said system configured to generate a new communications key using a secret value stored in said unit,

- generate an update key using said secret value stored in said unit. (Column 2, lines 23-27), where the update key is SSDA, and SSDA is apart of SSD, generated using RANDSSD.
- generate a signature value using said update key, where the signature value is $CAVE_{SSDA}(Rm)$ (Column 2, lines 30-40)
- compare said signature value with a signature value received from a visiting communications system of said communications system which was generated by said visiting communications system using said update key derived by a home communications system of said communications system, where the signature values $CAVE_{SSDA}(Rm)$ are compared at the mobile. (Column 2, lines 42-46)
- update said communications key with said new communications key depending on the results of said comparison, where if the results of the comparison are correct, then both side are authenticated and the communications key will be updated. (Column 2, lines 57-58)

In reference to claim 17:

Patel(Column 1, Line 40 – Column 2, line 58) discloses a key update system for updating a communications key maintained in a unit and in a communications system, said system configured to receive from a home communications system an update sequence and an update key derived by said home communications system using a secret value associated with said unit and stored in said home communications system, (where the update key is SSDA, and the home communications system is the AC/HLR) (Column 2, lines 22-32)

- to send to said unit said update sequence for said unit to generate a new communications key using a secret value in said unit, to generate a signature value at said visiting communications system using said update key derived by said home communications system,

  where the update sequence SR is sent to the unit to generate a new communications key SSDB (Column 2, lines 57-58), and to generate a signature value $CAVE_{SSDA}(Rm)$ using the update key SSDA. (Column 2, lines 20-45)
- to send to said unit said signature value for said unit to compare with a signature value generated at said unit using an update key generated by said unit using said secret value stored in said unit, where the signature value $CAVE_{SSDA}(Rm)$ is sent to the mobile to be compared with the $CAVE_{SSDA}(Rm)$ calculated and stored by the mobile. (Column 2, lines 42-46)
- to receive an update confirmation depending on the results of said comparison, where if the results of the comparison are correct, then both side are authenticated and the communications key will be updated. (Column 2, lines 57-58)

In reference to claim 18:

Patel(Column 1, Line 40 – Column 2, line 58) discloses a key update system for updating a communications key maintained in a unit and in a communications system, said system configured to generate an update sequence,

- to generate a new communications key using a secret value stored in said system and associated with said unit, where the new communications key is a new session key generated using the secret values RANDSSD, Rn, Rn, SSDA, SSDB. (Column 2, lines 57-58)
- to generate an update key using said secret value, to send said update key to a visiting communications system for said visiting communications system to generate a signature value which is sent to said unit for comparison to a signature value generated at said unit using an update key generated at said unit using a secret value stored in said unit, where the update key generated is SSDA, the secret value used is RANDSSD, the update key is sent to a visiting communications system, VLR, where the VLR generates a signature value $CAVE_{SSDA}(Rm)$, where $CAVE_{SSDA}(Rm)$ is sent to a unit, the mobile unit for comparison to $CAVE_{SSDA}(Rm)$ generated by the mobile unit using a secret value stored in said unit RANDSSD. (Column 2, lines 20-46)
- to update said communications key with said new communications key depending on the results of said comparison, where if the results of the comparison are correct, then both side are authenticated and the communications key will be updated. (Column 2, lines 57-58)

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TMH

March 8th, 2004